DOI: 10.38146/BSZ.2018.7-8.8

HERÉDI ISTVÁN

Nyílt forrású adatgyűjtés az interneten

Napjainkban különleges médiafigyelem övezi az internetes közösségimédia-felületek adatkezelési gyakorlatát. A közösségimédia-szolgáltatók nyíltan hozzáférhető felületet kínálnak, amelyre regisztrálva – és alapvető személyes adatainkat megadva – szöveges vagy grafikus tartalmakat oszthatunk meg, híreket, cikkeket olvashatunk, ismerősöket gyűjthetünk, illetve figyelemmel kísérhetjük a mások által megosztott tartalmakat is.

Az okostelefonok és egyéb okoseszközök világában meg sem lepődünk azon, hogy az egyik alkalmazás használatakor közvetlenül betöltődnek egy teljesen másik alkalmazásban használt adataink, esetleg közvetlenül ezeket felhasználva regisztrálhatunk az adott szolgáltatásra. Az okoseszközök rendkívül sok kényelmi funkcióval próbálják meg kellemesebbé tenni az életünket, illetve felgyorsítani az igényelt szolgáltatások elérését – aminek felhasználói szempontból természetesen rendkívül sok előnye van, mindamellett sok járulékos, személyes adat megosztására is sor kerül ezek használatával.

Az ilyen alkalmazások, médiafelületek és szolgáltatások használata általában ingyenes, vagy relatíve alacsony előfizetési díj ellenében vehető igénybe. Természetesen ez a szolgáltatók elsődleges érdeke is, hiszen – más gazdasági társaságokhoz hasonlóan – a profitmaximalizálás egyszerű reklámelhelyezéssel nem feltétlenül kivitelezhető. A célzott marketing, illetve fogyasztói csoportok gyűjtése azonban annál több haszonnal kecsegtet. Ez csak úgy valósítható meg, ha a szolgáltatók megfelelően ismerik felhasználóikat, ez pedig minél több releváns adat begyűjtése révén lehetséges.

A begyűjtött adatok a felhasználó által is publikusan elérhetővé, megjeleníthetővé tehetők, vagy akár háttér-információként kerülhet sor a felhasználásukra a célzott marketingkommunikáció keretében. Ezt a felhasználási kört igyekszik szabályozni az új európai uniós adatvédelmi rendelet, a GDPR is, amely az utóbbi időben kiemelt médiafigyelmet kapott.

A közösségi média és egyes alkalmazások használata természetesen csak egy-egy – bár kétségkívül hatalmas – szeletét teszi ki az interneten elérhető személyes, illetve meghatározott személyekhez köthető adatoknak. Eme adatforrások felkutatása és kiaknázása a nyílt internetes adatgyűjtés elsődle-

ges célja, ami bárki számára hozzáférhető forrásokból teszi lehetővé a releváns, célszemélyhez vagy célobjektumhoz köthető információk beszerzését.

A digitális lábnyom

Az internetet böngészve hatalmas mennyiségű adatot tehetünk rendkívül gyorsan megjeleníthetővé, akár a mobileszközünkről is. A böngészési tevékenység közben azonban egy sor algoritmus dolgozik azon, hogy a megfelelő tartalom jelenjen meg az eszközünk kijelzőjén, illetve az érdeklődésünknek megfelelő további tartalmakat ajánlhasson a szolgáltató. Minden egyes kattintás vagy billentyűleütés naplózható részfolyamatként jelenik meg a szerverek oldalán, így egy egyszerű weblap megtekintése is naplóbejegyzést generál.

Az adott weboldal üzemeltetője a naplóállományok alapján tudja megállapítani, hogy mikor, milyen IP-címről, milyen eszköz és böngészőszoftver felhasználásával és milyen tartalomhoz fértek hozzá. A nyomozó hatóság tagja az ilyen szerver-naplóállományokkal elsősorban az információs rendszereket is érintő bűncselekmények esetén lefoglaláskor vagy egy-egy üzemeltetői megkeresésre adott válaszban találkozhat.

Az ilyen böngészési adatokhoz – normális esetben – csak az oldal üzemeltetője, illetve a szerverszolgáltató férhet hozzá. Azonban a „minimális internetes aktivitás" elve alapján, ha akár egyetlen egyéb e-mail-fiókkal, szolgáltatásfelhasználói hozzáféréssel vagy profillal bír, akkor valószínűsíthetően egyéb olyan online aktivitás is köthető hozzá, amely a már meglévő profilt egy másik szolgáltatáshoz társítja. Erre a legegyszerűbb példa egy webshop, hirdetési felület, hírfolyam vagy bármely alapvető szolgáltatás használata, amely e-mail-címhez kötött, így a felhasználó regisztrációkor a hozzáféréséhez társítja a levelezőfiókját.

Az online tevékenységünk során tehát egy sor olyan adat képződik, amely ha csak megfelelő hozzáférési jogosultsággal is, de visszavezethető hozzánk. Az internet böngészése során így gyakorlatilag egy digitális lábnyom keletkezik, amelyet visszakövetve a személyre vonatkozó közvetlen és közvetett információk gyűjthetők össze.

A nyílt forrású adatgyűjtés – angol szakkifejezéssel Open Source Intelligence, röviden OSINT – elsődleges célja olyan, nyílt forrásokból származó információk felkutatása és abból értékelhető adathalmazok kinyerése, ami a célszemélyre vagy célobjektumra vonatkozólag információtartalommal bír.

Az adatgyűjtés nyílt jellegére tekintettel az bárki által elvégezhető, külön szakképzettséget vagy szaktudást nem igényel, sokkal inkább gyakorlatot vagy az online szolgáltatások használatában való jártasságot feltételez.

Természetesen a nyílt forrású adatgyűjtésen elsősorban az online felkutatható adatforrásokból beszerezhető információkat értjük, hiszen a technikai fejlődés lehetővé tette ezzel a módszerrel nagy mennyiségű adat egyidejű, gyors és egyszerű beszerzését. Ennek analógiájára természetesen klasszikus offline források is kutathatók, amire a legegyszerűbb példa egy telefonkönyv. A telefonkönyvben az egyes körzetekhez – azaz településekhez – társítva személyneveket, lakcímeket, illetve az e szolgáltatási helyhez tartozó telefonszámokat találhatjuk meg. Az adatgyűjtés így csupán ennek az egy forrásnak az ismeretében is egyetlen adat – amely akár a célszemély neve, lakcíme, vagy hívószáma – vonatkozásában két további, releváns információt hordozó adat megismerését vonja maga után.

A nyílt forrású adatgyűjtés leginkább egy Rubik-kocka kirakásához hasonlítható. A különböző szolgáltatási felületeken elérhető adatokat csoportosítva, majd megfelelően rendezve felépíthető a célszemély online profilja. A személyes adatokon kívül a célszemélyhez köthető további olyan információk is elérhetők lehetnek, mint a személy ismeretségi körére, otthonára, körülményeire, családtagjaira, felhasználási szokásaira, mozgására, érdeklődési körére vonatkozó adathalmazok.

Azt, hogy egy adott személyre milyen adatok vonatkozásában kereshetünk az interneten, leginkább online aktivitása határozza meg. Ha a célszemély csupán egyetlen e-mail-fiókot használ és semmilyen más módon nem aktív az interneten, akkor valószínűleg az e-mail-fióktól eltérő források kutatása nem vezet eredményre. Ez azonban nem minden esetben igaz. Elképzelhető, hogy nem maga a célszemély osztja meg az – adatgyűjtésünk szempontjából releváns – információt, hanem valamely ismerőse, esetleg valamely harmadik fél, vagy egyszerűen nyílt módon hozzáférhető adatbázisban szerepel. A digitalizáció világában így kifejezetten ritka az az eset, amikor valakivel kapcsolatban abszolút semmilyen információforrás nem kutatható fel az interneten. Az ilyen esetek vagy tudatos és alapos távolmaradást feltételeznek, vagy a célszemély és környezete valóban nem szerepel sem szolgáltatások felhasználójaként, sem elektronikus adatbázisokban rögzített objektumként.

Az információ forrásai lehetnek tehát a nyilvános adattárak, a közösségi profilok, az online médiaszolgáltatók, a hírforrások, hirdetési felületek, saját feltöltött tartalmak, illetve összességében bármely, a tartalomszolgáltatók által rendelkezésre bocsátott felületeken nyílt módon elérhető adathalmaz is.

Felderítési lehetőségek

A nyílt forrású adatgyűjtés nem közvetlenül a kiberbűncselekmények felderítéséhez köthető járulékos cselekménysor, hiszen az a „klasszikus" bűncselekményeket elkövető személyek esetében hasonló hatékonysággal végezhető.

Az elsődleges felderítés a legtöbbször valamely kezdeti információ vagy annak töredéke birtokában kezdődik, és közvetlen célja a rendelkezésre álló információhalmaz bővítése. A folyamatban lévő eljárások bármely szakaszában bevezethető cselekménysorról beszélhetünk, hiszen akár annak kezdeti szakaszában, akár később az eljárás folyamán bármikor szükség lehet a releváns információk összegyűjtésére.

Az adatgyűjtés elsődleges célja a célszemély vagy személyi kör, esetleg más releváns személyek vagy célobjektum beazonosítása, és róluk a lehető legtöbb információ összegyűjtése. Az így beszerzett információk tekintetében megkereséssel élhetünk akár a tartalomszolgáltatók, akár a hírközlési szolgáltatók irányába, így lehetővé válik a már személyhez köthető internetelőfizetés beazonosítása is. Az elvégzett adatgyűjtési tevékenység után további nyomozati cselekmények végrehajtása válhat szükségessé, amelynek során a beszerzett információk vonatkozásában aztán újabb, illetve további adatgyűjtésbe kezdhetünk. A folyamat addig ismétlődhet, amíg az eljárásban azonosítandó valamennyi személy, esemény, objektum és körülmény beazonosítása megtörténik.

Fontos tehát kiemelni, hogy a nyílt forrású adatgyűjtés nem csupán önmagában, hanem más, „klasszikus" eljárási cselekmények egyidejű alkalmazásával érheti el hatékonyságának legmagasabb fokát, hiszen a nyílt módon beszerezhető információk tekintetében a hatóságot megilleti az a „luxus", hogy azokat nyilvántartásokban ellenőrizze, illetve azok tekintetében megkereséssel éljen.

Az információ forrása gyakorlatilag bármi lehet. Az egyes tartalomszolgáltatók felületén elérhető keresési opciók bemutatása külön leiratot igényelne, hiszen mind a felületek számának növekedésével, mind pedig a megosztott információk és tartalmak egyre intenzívebb megjelenítésével az elérhető keresési lehetőségek száma is drasztikusan emelkedett.

A keresések legjelentősebb részét nagy valószínűséggel a személyes közösségi profilok teszik ki, hiszen az adatgyűjtések nagy része fókuszál célszemélyek beazonosítására. Az ilyen keresések végrehajtásához leginkább gyakorlat, semmint különleges szakértelem szükséges. Az elérhető keresési opciók azonban gyakran változnak, hiszen a tartalomszolgáltatók is fejlesztik szolgáltatásaik motorját, így azt rendszeresen érdemes figyelemmel kísérni.

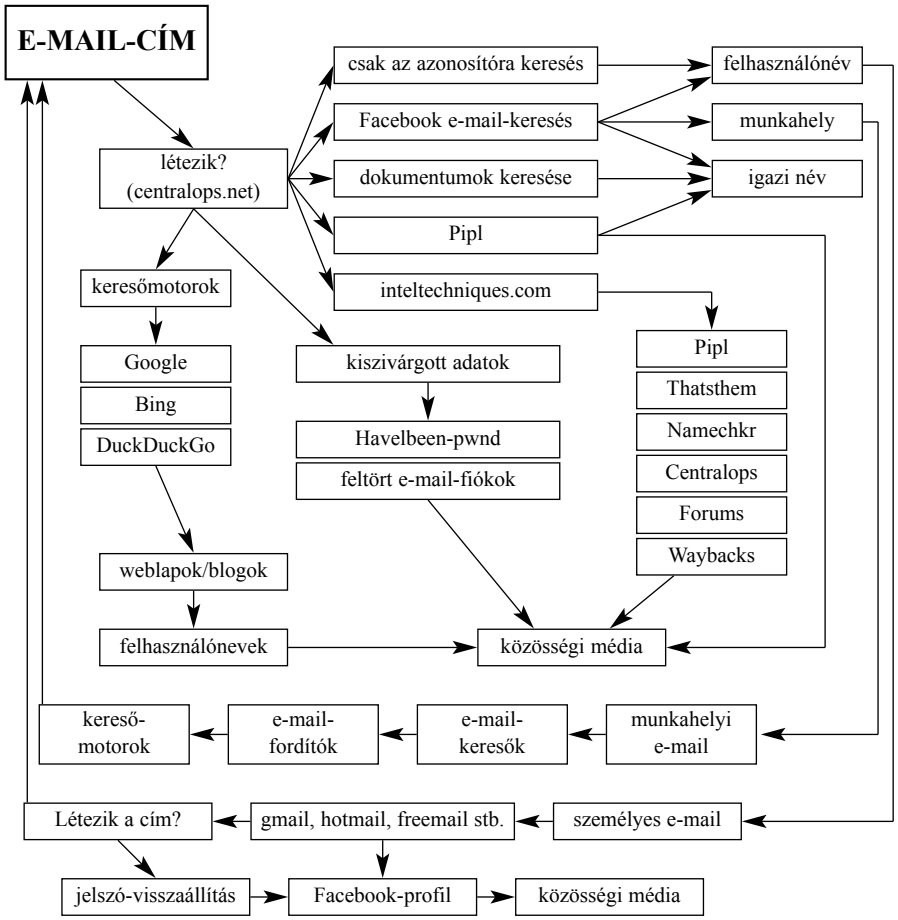
Aktív és passzív felderítés

Az interneten elérhető tartalmak többsége mára dinamikus tartalommá vált, ennek keretében nem csupán statikus jellegű weblapok jeleníthetők meg, hanem az egyes felületek akár felhasználónként is külön-külön személyre szabhatók. Ennek következménye, hogy nem ugyanazok a hirdetések jelennek meg mindenki számára a közösségi médiában – hanem leginkább az érdeklődési körünknek megfelelő, célzott reklámok –, illetve hogy az ilyen médiafelületeken különböző, személyre szabható profilokat lehet létrehozni.

A technológia előnye azonban egyben az adatgyűjtés bizonyos szempontú hátrányát is jelenti számunkra, hiszen korlátozható az elérhető, megjeleníthető tartalmak köre. Ha a célszemélynek privát vagy részben privát profilja van, csak akkor érhetjük el a lehető legtöbb informatív tartalmat, ha kapcsolatba kerülünk a profiltulajdonossal. A kapcsolatba kerülés itt jelentheti az adott profil követését, illetve akár azt is, hogy a személyt meg kell jelölnünk ismerősként. Semmi sem garantálja, hogy az elérhető tartalmak köre változni fog, nagyobb információmennyiség lesz elérhető, vagy hogy ezek közül bármelyik is releváns lesz az adatgyűjtés szempontjából. Az azonban teljesen biztos, hogy erről az aktivitásról a felhasználó értesítést kap. Ez az a lépés, ami az aktív és a passzív adatgyűjtés határát jelenti. A passzív adatgyűjtés során a célszemély nem értesül arról, hogy személye tekintetében információgyűjtés folyik. Az aktív adatgyűjtés esetében azonban már közvetlen vagy közvetett értesítéssel kell számolni, ami akár az adatgyűjtés dekonspirációjához is vezethet.

Az adatgyűjtés megkezdése előtt érdemes áttekinteni, hogy a célszemélynek milyen profiljai vannak, milyen információforrások állnak rendelkezésre, és az egyes forrásokból beszerezhető információk aktív vagy passzív tevékenységet feltételeznek-e. Külön ki kell térni arra a döntésre is, hogy a kizárólag aktív módszerrel beszerezhető információk „értéke” felülmúlja-e az adatgyűjtési tevékenység esetleges kompromittálódását.

A legegyszerűbben folyamatábrák felhasználásával lehetséges célirányos és tervezett adatgyűjtést végezni. A folyamatábra a felderítési vonatkozások és körülmények függvényében egyedileg alakítható ki – azonban természetesen léteznek általános érvényű munkafolyamatok is. Az *ábra* az e-mailek tekintetében végezhető adatgyűjtés gyakorlati algoritmusát mutatja. A vázlat megértéséhez természetesen szükséges az alapvető keresési lehetőségek ismerete is, azonban itt sokkal inkább a keresési folyamat szemléltetése a lényeg, amellyel a keresés így minden esetben mechanikus folyamat része lesz, így a hiba kockázata minimálisra csökkenthető.



Az elérhető adatok köre szolgáltatónként és felületenként is más és más, így azok kidolgozása, illetve a módszerek felderítése is külön figyelmet igényel. Fontos azonban, hogy információtartalmat nem csak a képi és szöveges adatok hordozhatnak. A célszemély megosztási szokásaiból közvetlen következtetéseket vonhatunk le egyéb online jelenlétére, online aktivitására is. Az információ hiánya is sok esetben árulkodó lehet, hiszen az használaton kívüli profilt, nem létező személyt fedő vagy egyéb konspirált tevékenységet folytató személyt feltételezhet. Az egyes adatgyűjtési lehetőségek kihasználása során így a beszerezhető információkon kívül a beszerzés, illetve a fellelhetőség körülményeire vonatkozóan is érdemes következtetéseket levonni, azzal kapcsolatban pedig verziókat felállítani.

Különös figyelemmel kell eljárni az olyan saját tartalmak esetében, mint amilyenek az egyedi weblapok, dinamikus tartalmak, átirányított hivatkozások, mivel ezek esetében az oldal üzemeltetője, illetve a tartalom tulajdonosa rendelkezhet webnaplókkal, amelyek rögzítik a beérkezett kéréseket. A legtöbb ilyen naplóállomány a digitális lábnyomnak megfelelően nemcsak az eszközről, de az internetkapcsolatról, illetve az esetleges átirányításokról is rögzít adatokat. Ilyen esetekben a kapcsolat és az eszköz elfedése tekintetében célszerű VPN-[1] vagy proxyszolgáltatások alkalmazása.

A felderítés passzív jellege csak konspirált hálózati kapcsolat, operációs rendszer, illetve online profil használatával biztosítható. Ha ezek közül az elemek közül bármelyik esetében nem gondoskodunk megfelelően online azonosságunk elfedéséről, akkor – módszertől függően eltérő mértékben ugyan, de – az adatgyűjtésünk felderíthetővé, így kompromittálóvá válik.

Adatgyűjtés a deep és dark weben

A nyílt interneten végezhető adatgyűjtés mellett egyre jelentősebb szerepet kap az internet „sötét oldalán" – a köznyelvben *dark weben* – végzett felderítőmunka. Ahhoz azonban, hogy eredményes adatgyűjtő munkát végezhessünk a *dark weben,* fontos tisztában lenni annak működési elvével, alapvetői fogalmaival is.

A nyílt internetes tartalom a *world wide web* mindenki által hozzáférhető, különböző doméncímeken elhelyezett adattartalmak összessége, amelyek megnyitásához több, ingyen hozzáférhető böngészőszoftver áll rendelkezésre. A domén- vagy IP-cím ismeretében e böngészők segítségével bármely – nyíltan hozzáférhető – felület megnyitható, tartalma böngészhető.

Ha a keresett adatokat tartalmazó weboldal pontos címét nem ismerjük, különféle keresőszolgáltatások felhasználásával rákereshetünk a számunkra releváns elemeket tartalmazó webhelyekre. A keresőmotorok olyan összetett algoritmusok, amelyek egy korábban már felállított indextartományon belül keresnek, majd a releváns kulcsszavakat tartalmazó találatokat megjelenítik a felhasználónak. Az indexelés keresőbotok felhasználásával történik, amelyek minden egyes nyíltan hozzáférhető weboldalt megnyitnak, majd az azo-

1 A VPN *(Virtual Private Network)* egy virtuálisan létrehozott privát hálózat, amelyhez kapcsolódva a hálózaton kívülre irányuló forgalom átirányítására titkosítva kerül sor az adatforgalom lebonyolításáért felelős szerveren keresztül. Használatával az internetes felületeken – normál körülmények között – csak a virtuális hálózatot kiszolgáló szerver fizikai és hálózati adatai jeleníthetők meg.

kon található összes hivatkozást tovább követve mintegy végigpásztázzák az internet teljes tartalmát.

Az egyes webhelyek rendszergazdáinak természetesen lehetőségük van arra is, hogy ezt a fajta indexelést, az oldal végigpásztázását letiltsák. Ez egyetlen fájl[2] webgyökérkönyvtárban történő elhelyezésével megoldható, és ez után a keresőbotok az oldalra jutva azt egyszerűen átugorják. Ezek az oldalak tehát a pontos domén- vagy IP-cím ismerete nélkül nem lesznek betölthetők, és az egyes keresőszolgáltatásokon keresztül sem lehetséges azokat elérni. Így alakul ki az internetes tartalmaknak az a tartománya, amelyet *deep webnek,* azaz *„sötét webnek”* neveznek.

A *dark net* bármely olyan hálózatot magában foglal, amely nem érhető el egyszerű, nyílt hozzáféréssel bárki számára. A *dark web* ezzel szemben az a webes tartalom, amely csak külön célszoftverrel – külön erre a célra programozott böngészők segítségével – nyitható meg. Az előbbi terminológiát alkalmazva a dark web a deep web része, azonban a kettő nem azonos egymással. A fogalmak elhatárolása fontos lépés, hiszen mind az adatgyűjtés technológiája, mind pedig annak módszerei különbözők a két eltérő felületen.

Az elérési útvonalak meghívására a dark web esetében nem a megszokott rendben, domén- vagy IP-cím alapján kerül sor, hanem a hivatkozások internetes felületen vagy egyéb módon történő közvetlen megosztásával.

Az ilyen tartalmak megnyitása nem lehetséges a hagyományos internetes böngészők segítségével, ahhoz külön célszoftverre van szükség. Attól függően, hogy melyik hálózathoz tartozó tartalmakat kívánjuk megnyitni, beszélhetünk egyebek között a *Tor-,* az *I2P-,* illetve a *Freenet-hálózatokról.* A legnépszerűbb felület az előzők közül a *Tor-hálózat,* amelynek megtekintéséhez, illetve webes felületének használatához a *Tor böngésző* szükséges.

A Tor böngésző egy – az ingyen hozzáférhető, szabadon szerkeszthető – Mozilla böngészőből átalakított speciális böngészőszoftver, amelynek segítségével az *.onion végződésű* hivatkozási címek megnyithatók.

Leegyszerűsítve a Tor-hálózat egy önkéntes alapon szerveződő hálózat az interneten belül, amelynek mára mintegy hétezer átirányítási pontja van. A hálózat lényege, hogy az arra kapcsolódó felhasználó egy átirányítási soron keresztül a világ különböző pontjain elhelyezkedő számítógépeken áthidalva kapcsolatát egy másik számítógépen – *a kilépési ponton* – keresztül kommunikál

2 A webgyökérkönyvtárban a „robots.txt” elnevezésű fájlt helyezik el, amely felsorolásszinten tartalmazza a letiltott könyvtárak jegyzékét. A fájl így információval szolgálhat arra, mely könyvtárakat nem szeretne az oldal üzemeltetője láthatóvá tenni a keresési felületeken.

az internetes szerverekkel. Az adatcsomagok a kiindulási és a kilépési pont között titkosítva közlekednek, ezáltal is növelve a felhasználó anonimitását.

A Tor-hálózat használatát egyes szolgáltatások jelzik, hiszen a Tor használata tényének elfedésére nem kerül sor. Ha a célszemély ezt a módszert használja, akkor csak az általa kilépési pontként használt számítógép IP-címét lehetséges egyszerű módszerekkel beazonosítani.

A dark weben megjeleníthető tartalmak köre teljes egészében megegyezik a nyílt internetes felületeken tapasztaltakkal, hiszen az oldalak ugyanúgy, böngészőben megjeleníthető statikus és dinamikus elemekből és objektumokból épülnek fel. A megosztott tartalmak jellege azonban eltérő. A nyílt interneten érvényesülnek az adott állami szabályozások a megjeleníthető tartalmak tekintetében, ezekre tekintettel nemzetközi egyezmények is születtek. A jogsértő tartalmakat így legtöbbször eltávolítják, illetve azok eltávolíthatók. A jogsértő tartalmak tekintetében is beszélhetünk azonban megtűrt, illetve meg nem tűrt tartalmakról. Előbbi kategóriába tartozik például a különböző hangfelvételek vagy filmek „kalózmásolatainak" megosztása, amely jogsértő tartalomnak minősül ugyan, mégsem minden esetben vonja maga után az eltávolítást és a közvetlen felelősségre vonást. A meg nem tűrt jogsértő tartalmak – amely például a gyermekek szexuális kizsákmányolásához kötődő grafikus elemek, illegális kábítószer- vagy fegyverkereskedelemhez köthető hirdetések – ellenben sokkal aktívabb ellenérzést váltanak ki, így eltávolításukról a legtöbb esetben gyorsan intézkednek. Az ilyen illegális tartalmaknak kínál kiváló lehetőséget a dark web, hiszen az oldal, illetve azok üzemeltetőinek beazonosítása jóval nehezebb, így anonim módon és relatíve egyszerűen válhatnak hozzáférhetővé a jogsértő tartalmak.

Természetesen a dark weben sem csupán jogsértő tartalmakkal találkozhatunk, azonban a relatíve szűkített felhasználószám kevéssé teszi kifizetődővé jogszerű tartalmak ilyen felületen történő elhelyezését. Az adatgyűjtés tehát itt a legtöbb esetben illegális tartalmak köré összpontosul, amely lehet akár megosztott jogsértő tartalom, akár eladásra kínált tiltott termék – amelyre a piacterek kínálnak kiváló lehetőséget. A dark weben – a felhasználók egyszerű beazonosítását elkerülendő – a legtöbb esetben nem szükséges sem a regisztrációhoz, sem az egyes tartalmak felhasználásához nyílt internetes hivatkozott tartalom, például e-mail-fiók. A felhasználó egy név–jelszó-páros megadásával egyszerűen férhet hozzá az itt elhelyezett tartalmakhoz, illetve oszthat meg saját tartalmakat.

Így a beazonosítás az ilyen felületeken nehezebb, mint a nyílt interneten. Az elsődleges cél így az adatgyűjtés nyílt internetes felületekre terelése, azaz

minél több olyan információ beszerzése, amelynek relevanciája lehet a „klaszszikus” weben. Ezek lehetnek a célszemély által használt felhasználónév, a publikus PGP-kulcsból[3] visszafejthető e-mail-cím, a profilban megadott profilkép, illetve bármilyen más megosztott tartalom. A beszerzett adatok tekintetében aztán a nyílt interneten folytatott adatgyűjtésnek megfelelően következhetnek az egyes felderítési lépések.

A beszerzett információk értékelése

Az interneten elérhető információk sok esetben nem valós tartalmúak. Az adatgyűjtés során mindenképpen figyelembe kell venni az információ és az információ forrásának megbízhatóságát is. A felderítési munka tekintetében tehát fel kell állítani a

– megbízható és megerősített;
– megbízható, de meg nem erősített;
– nem megbízható, de megerősített;
– nem megbízható és meg sem erősített; valamint
– a bizonytalan informatív tartalmú információk kategóriáját.

Az egyes információforrásokat, illetve magukat az információkat is természetesen további megbízhatósági csoportokba lehet sorolni – akár a már jól ismert kategóriák szerint –, ami alapján a besorolási kategória is szélesedik.

Az adatgyűjtés jelentéssel vagy jegyzőkönyvvel zárul, amelyben a felderítési technikákat nem, csak a már beszerzett információkat, illetve azok forrását tüntetik fel. Mind a forrás, mind pedig az információtartalom tekintetében célszerű a megbízhatósági osztályok felállítása, és az annak megfelelő besorolás elvégzése, így a jelentést kézhez kapó személy átfogó képet kaphat az adatgyűjtésről. Az értékelés soha nem szubjektív értékítélet alapján történik, hanem az objektív besorolás alapján, amelyeket összegezve a jelentés egésze is megbízhatósági jelöléssel látható el.

Az egyes információforrások, illetve az egyes célobjektumokat érintő adatgyűjtési tevékenységek akár jegyzőkönyvszerűen megalkotott jelentéssablonban is megjeleníthetők, ami rendkívül felgyorsítja a beszerzett információk későbbi feldolgozását, elemzését, illetve értékelését.

FELHASZNÁLT IRODALOM

Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser: Open Source Intelligence Investigation. Springer, Cham, 2016

Bazzell, Michael: Open Source Intelligence Techniques. 6th ed. Amazon Fulfillment, London, 2018